REMARKS

Claims 1-24 are pending in the present application. By this Response, claims 1, 4, 5, 7, 9, 12, 13, 15, 17, 20, 21 and 23 are amended. Claims 1, 9 and 17 are amended to incorporate subject matter from claims 7, 15 and 23. Claims 4, 5, 7, 12, 13, 15, 20, 21 and 23 are amended in view of the amendments to claims 1, 9 and 17. Reconsideration of the claims in view of the above amendments and the following remarks is respectfully requested.

I. Examiner Interview

Applicants thank Examiner Ho for the courtesies extended to Applicant's representative during the February 7, 2005 telephone interview. During the interview, the differences between the prior art and the presently claimed invention were discussed. Examiner Ho stated he would consider the arguments presented by the Applicant. The substance of the interview is summarized in the remarks of sections that follow.

II. 35 U.S.C. § 102, Alleged Anticipation, Claims 1-3, 6, 8, 9-11, 14, 16-19, 22 and 24

The Office Action rejects claims 1-3, 6, 8, 9-11, 14, 16-19, 22 and 24 under 35 U.S.C. § 102(b) as being anticipated by Weeks et al. "CCI-Based Web Security: A Design Using PGP." This rejection is respectfully traversed.

As to claims 1, 9 and 17, the Office Action states:

> In reference to claim 1:
> Weeks et al. discloses a method in a data processing system, said method comprising the steps of:
> - Receiving a request for a secure Web page, said secure web page including data, where the request for a secure webpage is website that has been encrypted with PGP. (Page 6-7, "Viewing PGP Enhanced Documents Using CCI")
> - Determining whether said data has been pre-encrypted, where it is known if the website has been encrypted with PGP if it has the

extension .pgp. (Page 6, "Storing PGP-Enhanced Documents as a Web Server")

- Bypassing an encryption step and transmitting said data in response to a determination that said data has been pre-encrypted, where the pgp file is served or transmitted to the client, if it has already been encrypted with PGP and has a .pgp extension. (Page 6-7, "Viewing PGP Enhanced Documents Using CCI")

Office Action dated November 18, 2004, pages 2-3.

Claims 9, 17 are rejected for the same reasons as claim 1.

Office Action dated November 18, 2004, page 4.

Claim 1, which is representative of the other rejected independent claims 9 and 17 with regard to similarly recited subject matter, reads as follows:

> 1. A method in a data processing system, said method comprising the steps of:
>
> receiving a request from a client for a secure Web page at a server, said secure Web page including data;
>
> establishing a secure session between said client and said server in response to said client transmitting said request;
>
> associating a cache with said secure session;
>
> determining whether a pre-encrypted version of said data has been stored in said cache in response to said receipt of said request; and
>
> in response to a determination that said pre-encrypted version of said data has been stored in said cache, transmitting said pre-encrypted version of said data.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re bond*, 910 F .2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 21 U.S.P.Q.2d 1031, 1034 (Fed Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. Kalman v. Kimberly-Clark Corp., 713 F .2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicant respectfully submits that Weeks does not teach every element of the claimed invention arranged as they are in the claims. Specifically, Weeks does not teach establishing a secure session between said client and said server in response to said client transmitting said request; associating a cache with said secure session; determining whether a pre-

encrypted version of said data has been stored in said cache in response to said receipt of said request; and in response to a determination that said pre-encrypted version of said data has been stored in said cache, transmitting said pre-encrypted version of said data.

Weeks is directed to the use of a general-purpose Common Client Interface (CCI) for enhancing the security of communications on the World Wide Web (WWW). In this approach, the Web browser communicates with an external CCI application that handles the processing of digitally-signed and/or encrypted data. Weeks' particular design uses the popular Pretty Good Privacy (PGP) software for all cryptographic operations. Weeks defines a PGP-CCI protocol which can be used to protect any HTTP message exchange, and also describes a simpler scheme for PGP-protected form submissions (HTTP POSTs) which may be implemented without modifying web servers. Additionally, Weeks also discusses the advantage of using a PGP-CCI application to handle pre-encrypted/signed Web documents in a user-friendly manner.

Weeks does not teach establishing a secure session between said client and said server in response to said client transmitting said request. The Office Action acknowledges that Weeks does not teach this feature. However, since claims 1, 9 and 17 now include subject matter previously rejected under the combination of Weeks and the Examiner's Official Notice, the Office Action states:

> The Examiner takes official notice that the use of SSL, or the Secure Sockets Layer was well known in the art in the time of invention. Secure Sockets Layer is a well known protocol widely used in Internet transactions because of its balance with respect to speed and security. E-commerce websites and banks that use SSL all employ the https:// as opposed to http://. To this effect, the use of SSL is ubiquitous.

Applicants respectfully traverse the Examiner's Official Notice use in combination with the Weeks reference. Weeks specifically addresses using a Common Client Interface (CCI) which leverages the use of external applications to perform operations for the web application. Weeks does not address the use of secure session communications processing with the applications because Weeks has no knowledge of the information being passed through the HTTP connection. Weeks' system sits at the top of the application layer. Any encryption takes place before the information is passed through the HTTP or network layer. Thus, there is no need for, as the Examiner alleges, the use

of secure session communications in the Weeks system as the information is already encrypted. Moreover, Weeks specifically teaches a PGP-CCI protocol which can be used to protect any HTTP message exchange and a simpler scheme for PGP-protected form submissions which may be implemented without modifying web servers. Applicant's invention works at the top of the network layer, while getting "hints" from the application layer. Thus, while the use of a secure protocol is well known in the art, establishing a secure session between said client and said server in response to said client transmitting said request is not taught or suggested by Weeks and the Examiner's Official Notice, either alone or in combination.

Additionally, Weeks does not teach associating a cache with said secure session. The Office Action acknowledges that Weeks does not teach this feature; however, the Office Action states:

> It would have been obvious to one of ordinary skill in the art at the time of invention to use SSL in the web transactions between the client and the server and store accessed in data in a cache in order to encrypt the data transmitted in order to encrypt the data in such a way that was widely used and supported by the dominant web browsers, and leave in a location for faster access times in the near future.

The Office Action also states with regard claim 4 and the use of a cache:

> The Examiner takes official notice that storing encrypted data in a cache was well known in the art at the time of the invention. In fact, storing encrypted data in a cache is usually expected. A cache is a region of memory usually smaller than a regular of main block of memory of space, from which data will be frequently accessed. Cache is a memory concept, present in RAM, Hard Disk space, and processor memory, as a second storage used to quickly access data that has recently been retrieved. By the concept of temporal locality, a piece of information on a computer recently accessed, is likely to be accessed again in the near future. Caching the is action storing into the cache, information that has been accessed recently.

Applicants respectfully traverse the Examiner's Official Notice use in combination with the Weeks reference. As discussed above, Weeks does not teach a secure session and the Examiner's Official Notice with regard to the use of a secure protocol in the Weeks system is rooted in error as Weeks encrypts data prior to transmitting data across an HTTP connection and does not need additional security. Secure session communications

do not provide mechanisms to allow for pre-encryption of data that is sent over and over again. Web sites often have the same image used many places. In the present invention using this patent, the first time an image is sent over the secure session, it would be encrypted and placed in the cache. Then any subsequent pages that have the same image would use the previously encrypted cached copy, eliminating the encryption step. The association of the cache with a specific secure session is to ensure the separation of communications flows between different secure sessions. The present invention provides a transparent improvement to a server's secure session processing. Thus, while a cache is well known in the art, associating a cache with said secure session is not taught or suggested by Weeks and the Examiner's Official Notice either alone or in combination.

Furthermore, Weeks does not teach determining whether a pre-encrypted version of said data has been stored in said cache in response to said receipt of said request. The Office Action again acknowledges that Weeks does not teach this feature; however, the Office Action alleges that Weeks stores data in memory and cache is a memory. As discussed above, even if cache is a memory, the cache recognized by the Examiner is not a cache that is associated with a secure session. Thus, Weeks and the Examiner's Official Notice, taken alone or in combination, does not determine whether a pre-encrypted version of data has been stored in a cache associated with a secure session in response to the receipt of a request.

Still further, Weeks does not teach transmitting said pre-encrypted version of said data in response to a determination that said pre-encrypted version of said data has been stored in said cache. As discussed above, Weeks and the Examiner's Official Notice fail to teach a cache that is associated with a secure session. Thus, Weeks and the Examiner's Official Notice, taken alone or in combination, fail to teach transmitting a pre-encrypted version of data in response to a determination that the pre-encrypted version of the data has been stored in a cache associated with a secure session.

Thus, Weeks does not teach each and every feature of independent claims 1, 9 and 17 as is required under 35 U.S.C. § 102. At least by virtue of their dependency on independent claims 1, 9 and 17, the specific features of dependent claims 2-8, 10-16 and 18-24 are not taught by Weeks. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1-3, 6, 8-11, 14, 16-19, 22 and 24 under 35 U.S.C. § 102.

Furthermore, Weeks does not teach, suggest or give any incentive to make the needed changes to reach the presently claimed invention. Absent the Examiner pointing out some teaching or incentive to implement Weeks such that encryption is bypassed and transmitted in response to a determination that the document has been pre-encrypted, one of ordinary skill in the art would not be led to modify Weeks to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion or incentive to modify Weeks in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the Applicant's disclosure as a template to make the necessary changes to reach the claimed invention.

Moreover, neither Weeks nor the Examiner's Official Notice teaches or suggests the desirability of incorporating the subject matter of the other reference. That is, there is no motivation offered in either Weeks or the Official Notice for the alleged combination. The Office Action alleges that the motivation for the combination is "in order to encrypt the data transmitted in order to encrypt the data in such a way that was widely used and supported by the dominant web browsers, and leave in a location for faster access times in the near future." As discussed above, Weeks teaches an encryption method that encrypts data prior to sending it over the HTTP connection. The Examiner's Official Notice could not be incorporated into the Weeks reference. Thus, the only teaching or suggestion to even attempt the alleged combination is based on a prior knowledge of Applicant's claimed invention thereby constituting impermissible hindsight reconstruction using Applicant's own disclosure as a guide. One of ordinary skill in the art, being presented only with Weeks and the prior knowledge of a secure protocol and cache, and without having a prior knowledge of Applicant's claimed invention, would not have found it obvious to combine and modify Weeks to arrive at Applicant's claimed invention.

Moreover, in addition to their dependency from independent claims 1, 9 and 17, the specific features recited in dependent claims 2, 3, 6, 8, 10, 11, 14, 16, 18, 19, 22 and 24 are not taught by Weeks. For example, with regard to claims 6, 14 and 22, Weeks does not teach receiving a request for a secure Web page, where the secure Web page including static information and dynamically-changing information; determining whether the static information has been pre-encrypted; bypassing an encryption step and

transmitting the static information in response to a determination that the static information has been pre-encrypted; encrypting the dynamically-changing information; and transmitting the encrypted, dynamically-changing information. As discussed above, Weeks does not teach determining that data has not been pre-encrypted. Furthermore, Weeks does not teach determining if a web page contains either static or dynamically-changing. Nowhere, in any section of Weeks, is there a determination of the contents of a web page made, much less whether the contents are static and/or dynamic.

Therefore, in addition to being dependent on independent claims 1, 9 and 17, dependent claims 2, 3, 6, 8, 10, 11, 14, 16, 18, 19, 22 and 24 are also distinguishable over Weeks by virtue of the specific features recited in these claims. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 2, 3, 6, 8, 10, 11, 14, 16, 18, 19, 22 and 24 under 35 U.S.C. § 102.

III. 35 U.S.C. § 103, Alleged Obviousness, Claims 4, 5, 7, 12, 13, 15, 20, 21 and 23

The Office Action rejects claims 4, 5, 7, 12, 13, 15, 20, 21 and 23 under 35 U.S.C. § 103(a) as being unpatentable over Weeks et al. "CCI-Based Web Security: A Design Using PGP." This rejection is respectfully traversed.

Claims 4, 5, 7, 12, 13, 15, 20, 21 and 23 are dependent on independent claims 1, 9 and 17 and, thus, these claims distinguish over Weeks for at least the reasons noted above with regards to claims 1, 9 and 17. Moreover, Examiner's Official Notice does not provide for the deficiencies of Weeks and, thus, any alleged combination of Weeks and Examiner's Official Notice would not be sufficient to reject independent claims 1, 9 and 17 or claims 4, 5, 7, 12, 13, 15, 20, 21 and 23 by virtue of their dependency.

Moreover, in addition to their dependency from independent claims 1, 9 and 17, the specific features recited in dependent claims 4, 5, 7, 12, 13, 15, 20, 21 and 23 are not taught or suggested by Weeks and Examiner's Official Notice, either alone or in combination. With regard to claims 5, 13 and 21, the Office Action alleges that Weeks with the Examiner's Official Notice teaches or suggests in response to a determination that said pre-encrypted version is stored in said cache, bypassing the encryption step and transmitting said pre-encrypted version of the image; and in response to a determination

that said pre-encrypted version is not stored in said cache, encrypting said image and transmitting said encrypted image. Again, as discussed above, Weeks teaches transmitting pre-encrypted data in request to the client in response to a client requesting encrypted data. Weeks does not teach determining that a pre-encrypted version of the image exists, but, rather, encrypting data based on attributes sent in the request by the client.

Claims 7, 15 and 23 recite similar subject matter. That is claims 7, 15 and 23 recite "determining whether a pre-encrypted version of said data has been stored in said cache." Thus, in view of the above, Weeks and Examiner's Official Notice, taken either alone or in combination, fail to teach or suggest the specific features recited in independent claims 1, 9 and 17, from which claims 4, 5, 7, 12, 13, 15, 20, 21 and 23 depend. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 4, 5, 7, 12, 13, 15, 20, 21 and 23 under 35 U.S.C. § 103.

IV. Conclusion

It is respectfully urged that the subject application is patentable over the prior art of record and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: February 17, 2005

Francis Lammes
Reg. No. 55,353
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Agent for Applicant

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.